

FortiManager - AliCloud Cookbook

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 09, 2020

FortiManager 6.4 AliCloud Cookbook

02-640-619612-20200409

TABLE OF CONTENTS

About FortiManager for AliCloud	4
Instance type support	4
Region support	4
Models	5
Licensing	5
Creating a support account	5
Registering and downloading licenses	5
Deploying FortiManager on AliCloud	7
Obtaining the deployment image	7
Uploading the FortiManager installer to AliCloud	7
Configuring a virtual private cloud	10
Creating the FortiManager deployment image	11
Creating security groups	13
Creating an instance	15
Connecting to the FortiManager-VM	19
Security Fabric connector integration with AliCloud	21
Creating Fabric connector objects for AliCloud	21
Importing address names to a Fabric connector	22
Creating an IP address policy	22
Installing policy packages	23
Change log	25

About FortiManager for AliCloud

FortiManager provides security-operationalized visibility across your Fortinet Security Fabric and enables true security effectiveness and foresight to identify and understand the scope of threats. It also facilitates actionable responses and remediation of risks.

Quantifiable security solution information produces measurable accountability and uses those ratings to compare your security preparedness internally and to that of your industry peers.

Centralized change management helps you update policies and objects, maintain provisioning templates and easily configure changes to your APs, switches, SD-WAN and SDN connectors and more, to mitigate security events and apply configuration changes and policy updates.

Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), effectively applying policies and distributing content security/firmware updates. FortiManager is one of several versatile network security management products that provide diverse deployment types, growth flexibility, advanced customization through APIs, and simple licensing, all through central management and configuration.

Instance type support

You can deploy FortiManager for AliCloud as VM instances. Supported machine types may change without notice.

Region support

FortiManager-VM is available for purchase in all the regions/datacenters that the AliCloud global marketplace covers. Available regions are:

- Hong Kong
- Asia Pacific SE 1 (Singapore)
- US East 1 (Virginia)
- Asia Pacific NE 1 (Tokyo)
- US West 1 (Silicon Valley)
- EU Central 1 (Frankfurt)
- Middle East 1 (Dubai)
- Asia Pacific SE 2 (Sydney)
- Asia Pacific SE 3 (Kuala Lumpur)
- Asia Pacific SOU 1 (Mumbai)
- Asia Pacific SE 5 (Jakarta)
- North China 1
- North China 2
- China North 3 (Zhangjiakou)
- China North 5 (Huhehaote)

- East China 1
- East China 2
- South China 1

Models

FortiManager-VM is licensed based on the number of managed devices, amount of logging per day, and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as bring your own license (BYOL) models.

You can deploy FortiManager-VM using different CPU and RAM sizes and launch instances on various private and public cloud platforms.

Licensing

You must have a license to deploy FortiManager for AliCloud.

Creating a support account

To make use of Fortinet technical support and ensure products function properly, you must complete certain steps to activate your entitlement. The Fortinet support team can identify your registration in the system thereafter.

First, if you do not have a Fortinet account, you can [create one](#).

To create a support account:

1. Deploy and boot up the FortiManager-VM instance, and log in to the FortiManager GUI management console.
2. On the Dashboard, copy the VM serial number.
3. Go to [Fortinet Service & Support](#) and create a new account or log in with an existing account.
4. Go to *Asset > Register/Activate* to start the registration process.
5. In the *Specify Registration Code* field, enter the serial number, and select *Next* to continue registering the product. Enter your details in the other fields.
6. After completing registration, contact Fortinet Customer Support and provide the serial number for your FortiManager instance and the email address associated with your Fortinet account.

Registering and downloading licenses

After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

To register and download the license:

1. Go to [Fortinet Service & Support](#) and create a new account or log in with an existing account.
2. Go to *Asset > Register/Activate* to start the registration process. In the *Specify Registration Code field*, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-VM.
After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiManager-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Deploying FortiManager on AliCloud

Obtaining the deployment image

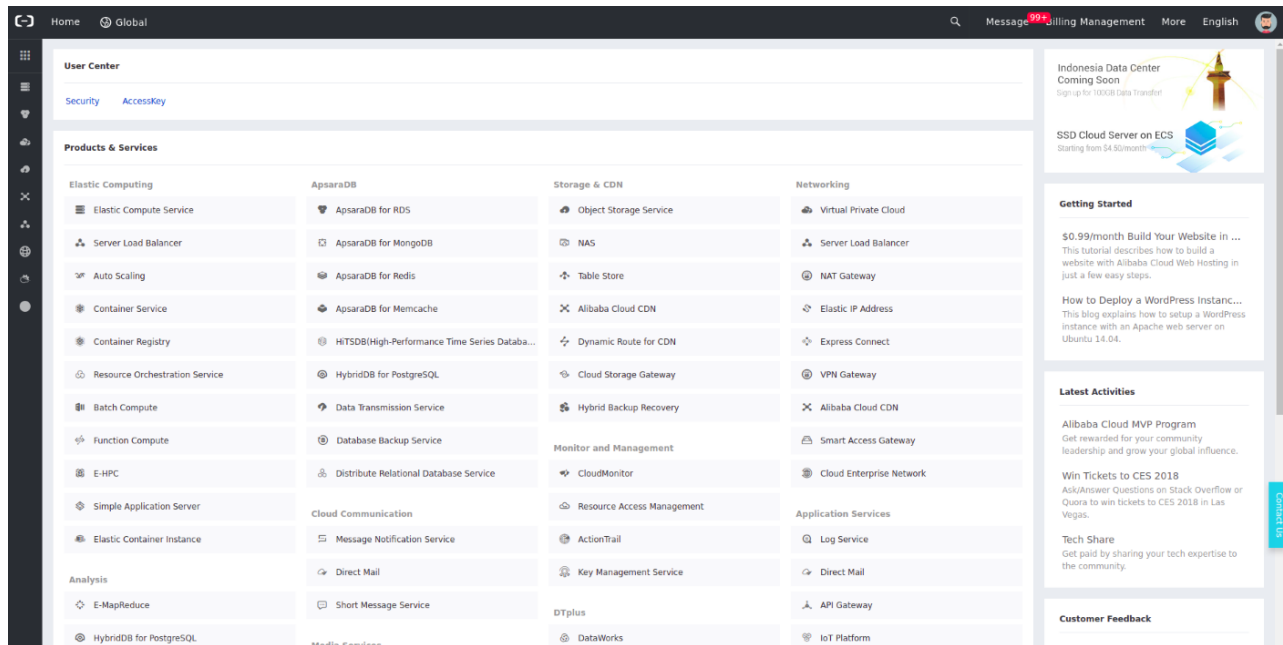
To obtain the deployment image:

1. Go to the [Fortinet support site](#) and log in.
2. Go to *Download > VM Images*.
3. Under *Select Product*, select FortiManager.
4. Under *Select Platform*, select *AliCloud*.
5. Download the deployment package file.

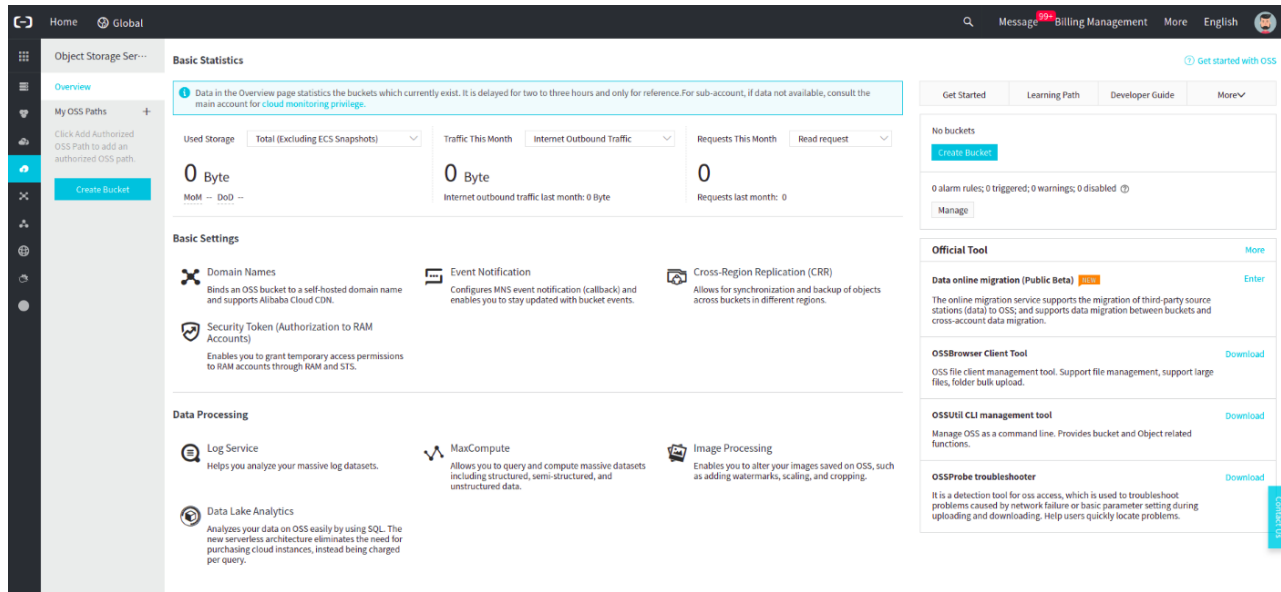
Uploading the FortiManager installer to AliCloud

To upload the FortiManager installer to AliCloud:

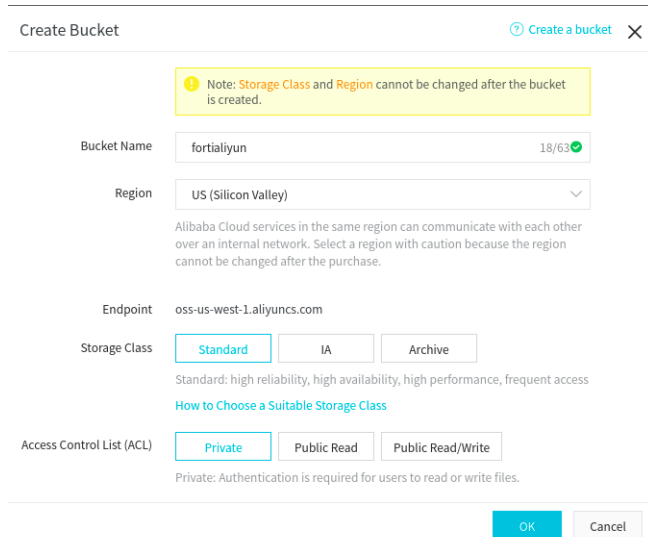
1. Log in to Alibaba Cloud.
2. Go to *Console > Object Storage Service*.



3. Click *Create Bucket*.



4. Configure the settings for the bucket and click *OK*.



5. Click the newly created bucket.

6. Click *Files*.

7. Click *Upload*.


8. Drag and drop the VM file to the bucket.

Upload X

Upload To Current Specified
 oss://fortialiyun/

File ACL Inherited from Bucket Private Public Read Public Read/Write
 Inherited from Bucket: The read/write permissions of each file are the same as those of the bucket.

Upload



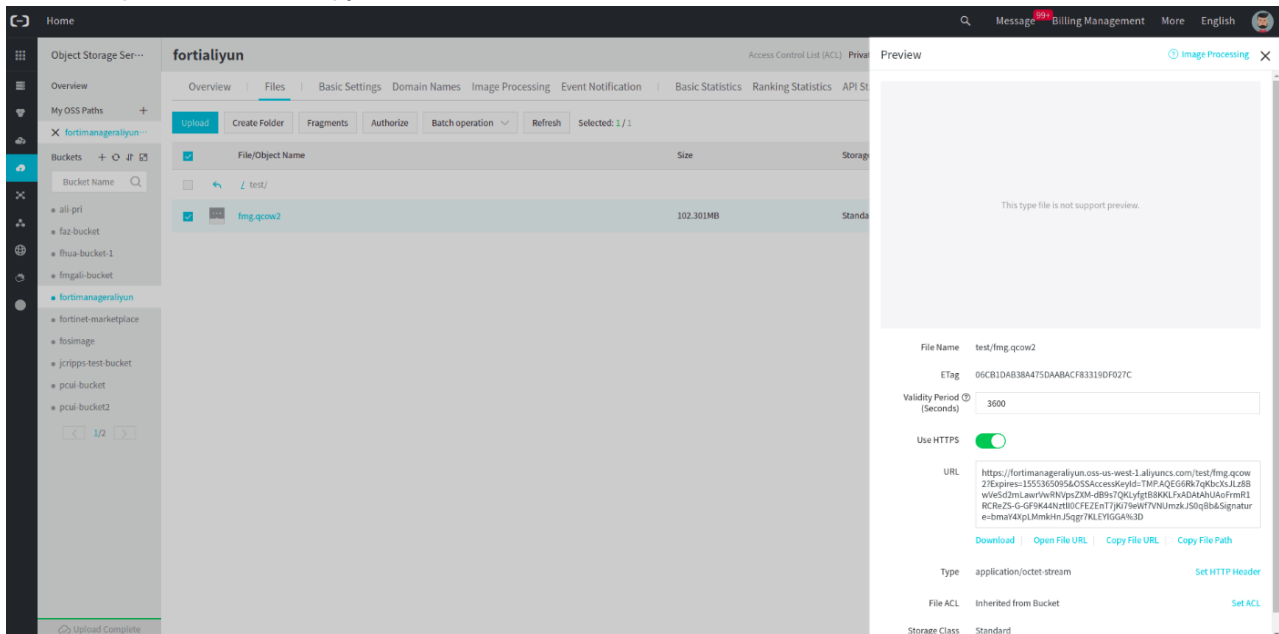
Drag and drop directories or files here, or
[click here to upload](#)
 Maximum 100 files

File naming rules:

1. Use UTF-8 encoding;
2. Case sensitive;
3. A name must be 1 to 1023 bytes in length;
4. A name cannot start with a slash / or consecutive backslashes \.

Note, file with the same name in the Bucket will be replaced by uploaded file.

9. Click the uploaded file and copy the URL.

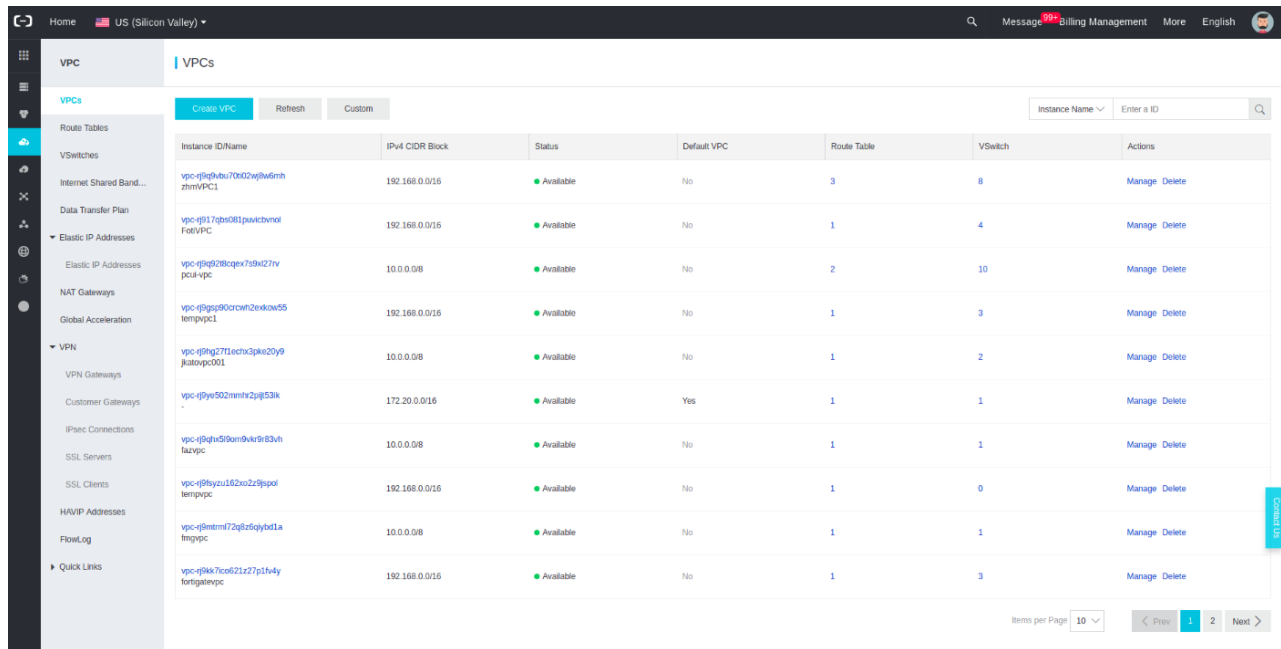


The screenshot shows the AliCloud console interface. On the left, a sidebar lists various buckets, with 'fortimanageraliyun' selected. The main area displays the 'fortialiyun' bucket contents, showing a file named 'fmg.qcow2' with a size of 102.301MB. A 'Preview' window is open on the right, showing the file details. The file name is 'test/fmg.qcow2', the ETag is '05CB1DAB38A475DAABACF83319DF027C', and the validity period is 3600 seconds. The 'Use HTTPS' option is checked. The URL is displayed as: `https://fortimanageraliyun.oss-us-west-1.aliyuncs.com/test/fmg.qcow2?Expires=1555305095&OSSAccessKeyId=TMPAQEG6R87qkbcXsJLz8BwWesD2mlawrtvRwRwpsZ3M-dB9s7QrLygt8BKKLFaDADANUoFmR1RC7aZs-G-6F9w4knt8BCEZExtTjpkWwT7NjmkzJ5Qqib6Signature-e-bma74kplMmkInJ5agr7KLEYtGG4%3D`. Below the URL, there are links for 'Download', 'Open File URL', 'Copy File URL', and 'Copy File Path'. The file type is 'application/octet-stream' and the storage class is 'Standard'.

Configuring a virtual private cloud

To configure a virtual private cloud:

1. Go to VPCs. Click *Create VPC*.



2. Enter a name for the virtual private cloud (VPC). Configure the settings as required and click **OK**.

Create VPC ✕

VPC

Region
US (Silicon Valley)

• Name ?
vpc 6/128 ✓

• IPv4 CIDR Block ?
192.168.0.0/16 ▼

ⓘ The CIDR cannot be changed once the VPC is created.

Description ?
 0/256

VSwitch

• Name ?
switch 9/128 ✓

• Zone ?
Silicon Valley Zone A ▼

Zone Resource ?
ECS ✓ RDS ✓ SLB ✓

• IPv4 CIDR Block
192 · 168 · 0 · 0 / 24 ▼

ⓘ The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs
252

Description ?

OK Cancel

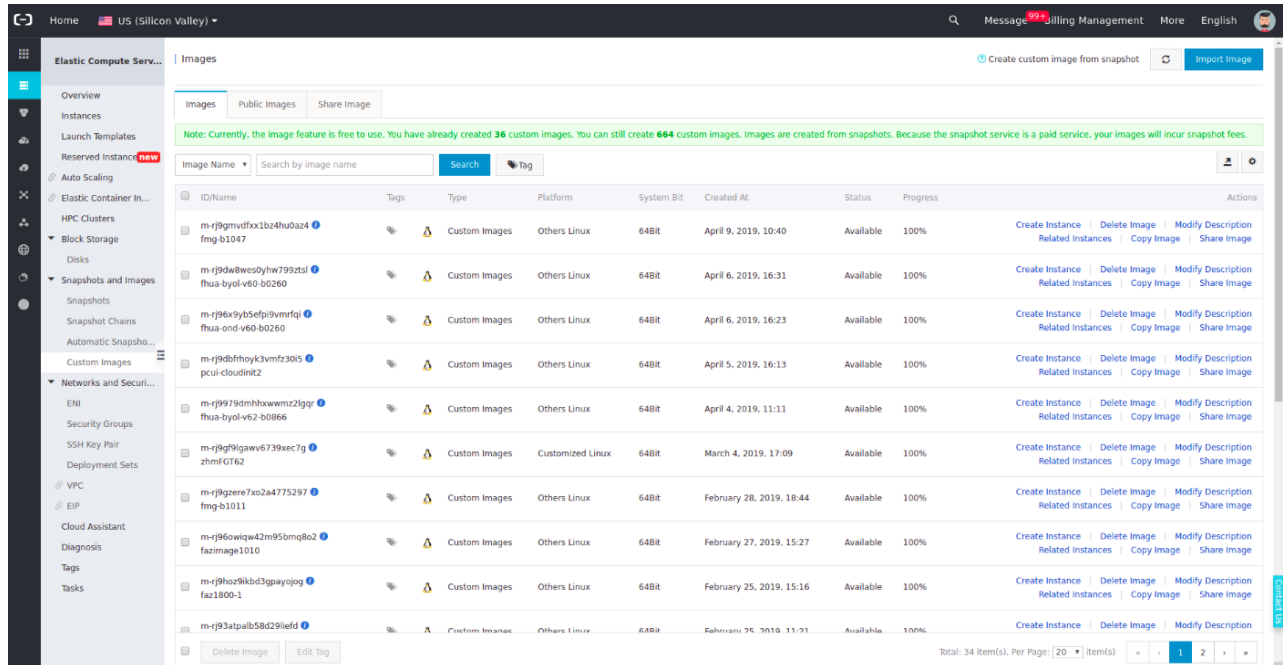
Contact Us

Creating the FortiManager deployment image

The following procedure applies only if you are uploading a custom image. To deploy FortiManager from the Marketplace directly, go to [Creating an instance on page 15](#).

To create the FortiManager deployment image:

1. Go to *Snapshot and Images > Custom Images*.



2. Click *Import Image*. Configure the settings in the Import Image screen. Configure the following settings:

- OSS Object Address - paste the URL from step 9 in [Uploading the FortiManager installer to AliCloud on page 7](#) into OSS Object Address.
- Image Name - specify a name for the image.
- Operating System - select *Linux*.
- System Disk Size - select the minimum disk size as *40 GB*.
- System Architecture - select *x86_64*.
- Platform - select *Other Linux*.
- Image Format - select *QCOW2*.

Import Image [Import custom image](#) ✕

When you create an image, a snapshot will be created at the same time. Because the snapshot service is a paid service, your images will incur snapshot fees.

How to import an image:

1. Perform the following: [Activate OSS](#)
2. Upload the image file to the bucket in the same region that the image will be imported to.
3. Make sure that you have authorized ECS to access your OSS. [Confirm Address](#)
4. Check if the image meets [Notes](#)

* Region of Image: US (Silicon Valley)

* OSS Object Address: [How to get the address of OSS files](#)

* Image Name:

* Operating System:

* System Disk Size (GB):
40 to 500 GB for Windows and 40 to 500 GB for Linux.

* System Architecture:

* Platform:

Image Format:

Image Description:

Add Data Disk Image

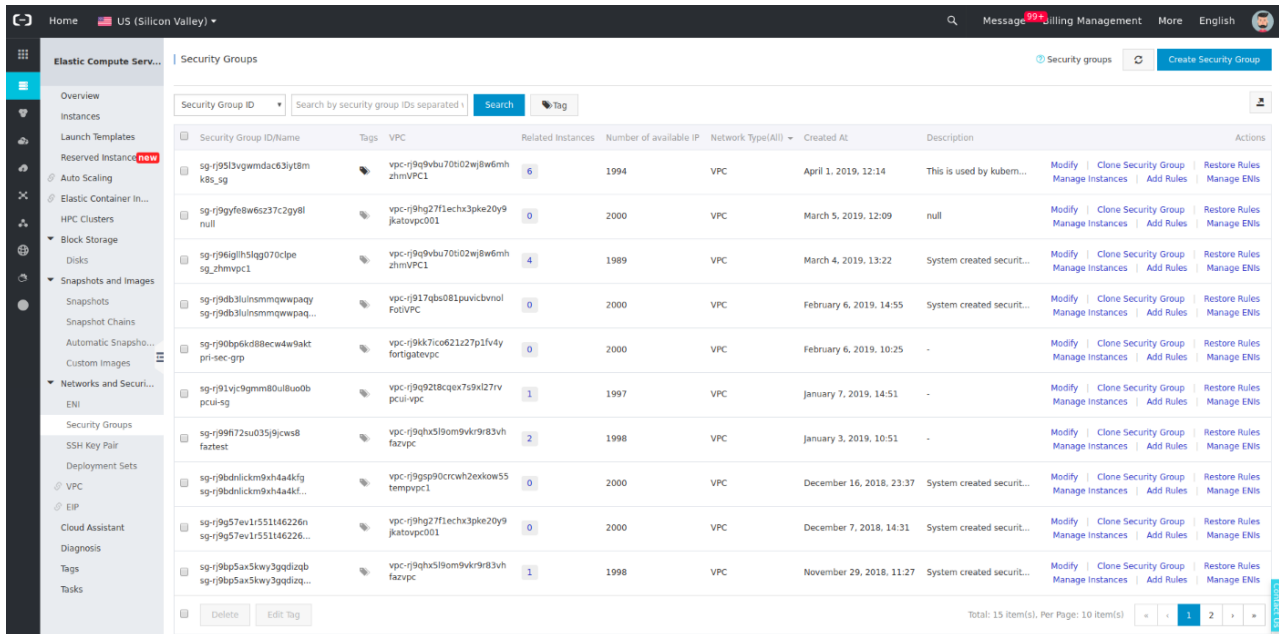
3. Click **OK**.

Creating security groups

To create security groups:

1. Go to *Elastic Compute Service > Network and Security*.
2. Click *Security Groups*.

3. Click *Create Security Group*.



4. Configure the security group and click *OK*.

Create Security Group Creating security group

Template: Web Server Linux

* Security Group Name: security-group-20190416
The name can be 2 to 128 characters in length and can contain periods (.), underscores (_), and hyphens (-). It cannot start with a special character or number.

Description: Security Group
It can be 2 to 256 characters in length and cannot start with http:// or https://.

Network Type: VPC

*VPC: vpc-rj917qbs081pucivbvnol [Create VPC](#)

Tag: Select a key or enter a new ... Select a value or enter a ne...

Ingress
Egress

Authorization Objects	Protocol Type	Port Range	Action
0.0.0.0/0	TCP	80/80	Allow
0.0.0.0/0	TCP	443/443	Allow
0.0.0.0/0	TCP	22/22	Allow
0.0.0.0/0	ICMP	-1/-1	Allow

OK
Cancel

5. Click *Create Rules Now*.

Notes ✕

! After creating a security group, we recommend that you immediately create security group rules. Otherwise, you may not be able to access the internal network or Internet.

Create Rules Now
Close

6. Click *Add Security Group Rule*.

Action	Protocol Type	Port Range	Authorization Type(All)	Authorization Objects	Description	Priority	Created At	Actions
Allow	Customized TCP	22/22	IPv4 CIDR Block	0.0.0.0/0	-	1	April 16, 2019, 12:04	Modify Clone Delete
Allow	Customized TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	-	1	April 16, 2019, 12:04	Modify Clone Delete
Allow	Customized TCP	80/80	IPv4 CIDR Block	0.0.0.0/0	-	1	April 16, 2019, 12:04	Modify Clone Delete
Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0.0/0	-	1	April 16, 2019, 12:04	Modify Clone Delete

7. Configure the settings as per your network infrastructure and click *OK*.

Add Security Group Rule ✕

NIC: Internal Network

Rule Direction: Ingress

Action: Allow

Protocol Type: Customized TCP

* Port Range: 80/80 ?

Priority: 1 ?

Authorization Type: IPv4 CIDR Bloc

* Authorization Objects: 0.0.0.0/0 ? Tutorial

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK
Cancel

Creating an instance

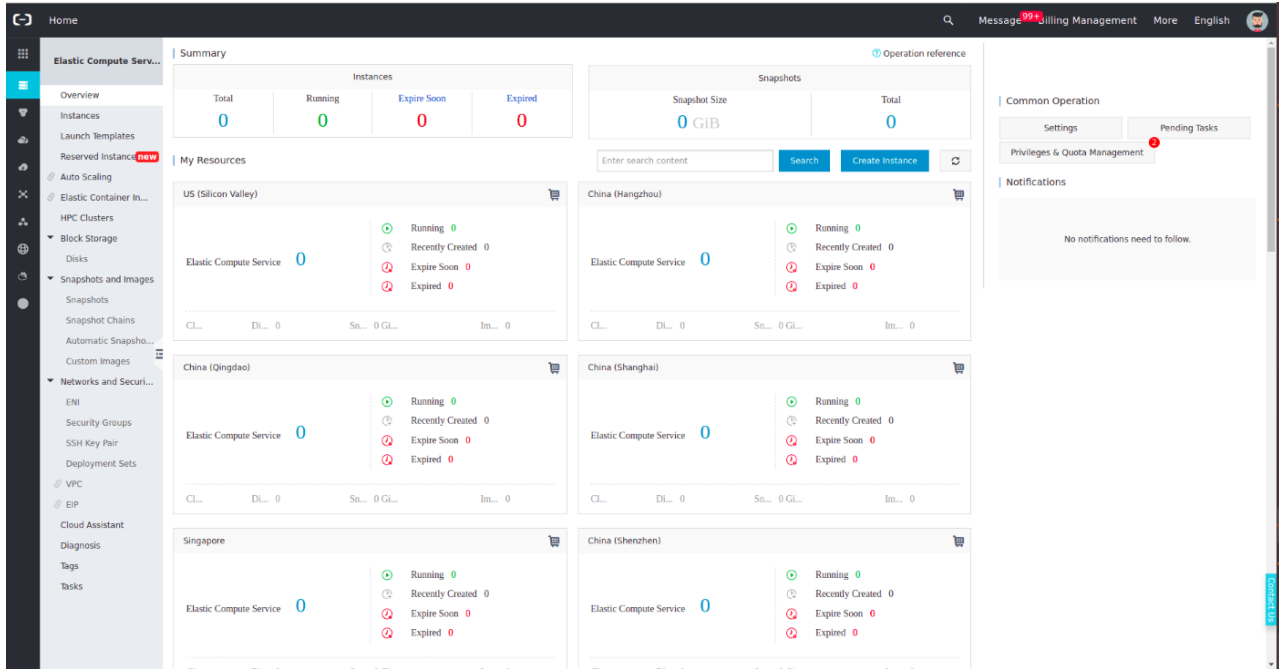
FortiManager can be deployed in the following ways:

- Go to *Alibaba Cloud > Marketplace* and choose FortiManager. Click *Choose Your Plan* and continue from step 2 described below.

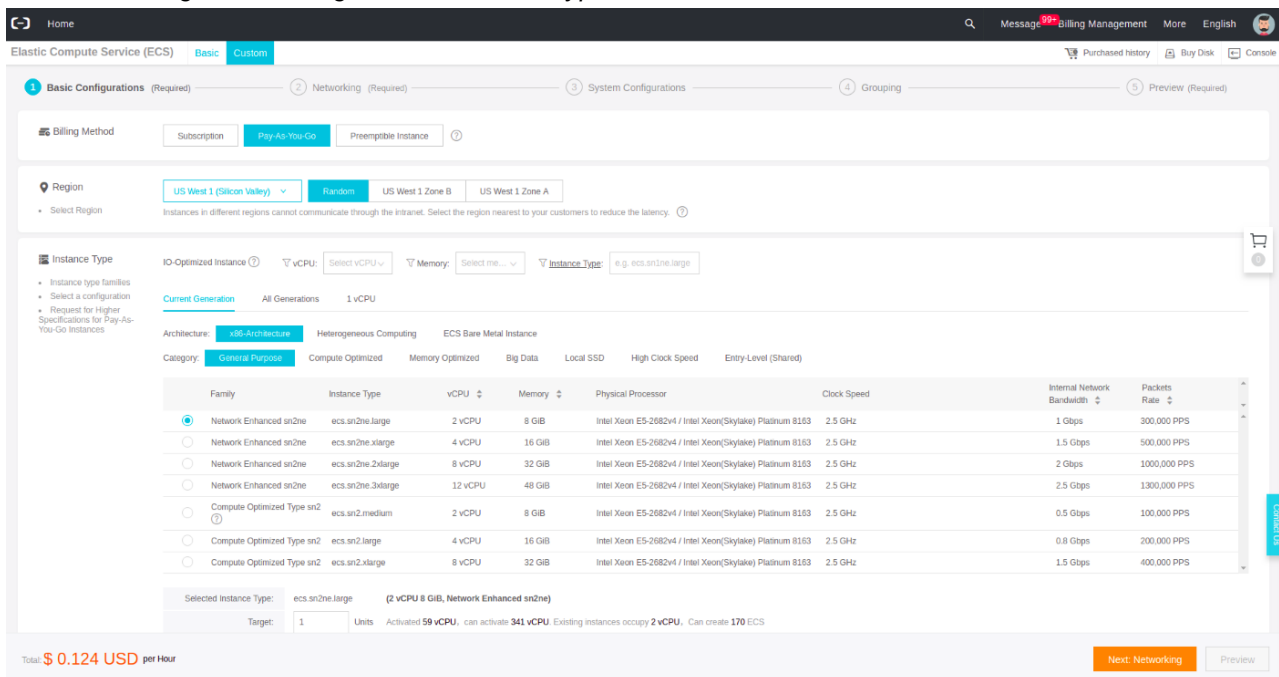
- Create a deployment image as described in [Creating the FortiManager deployment image on page 11](#) and follow the steps below.

To create an instance:

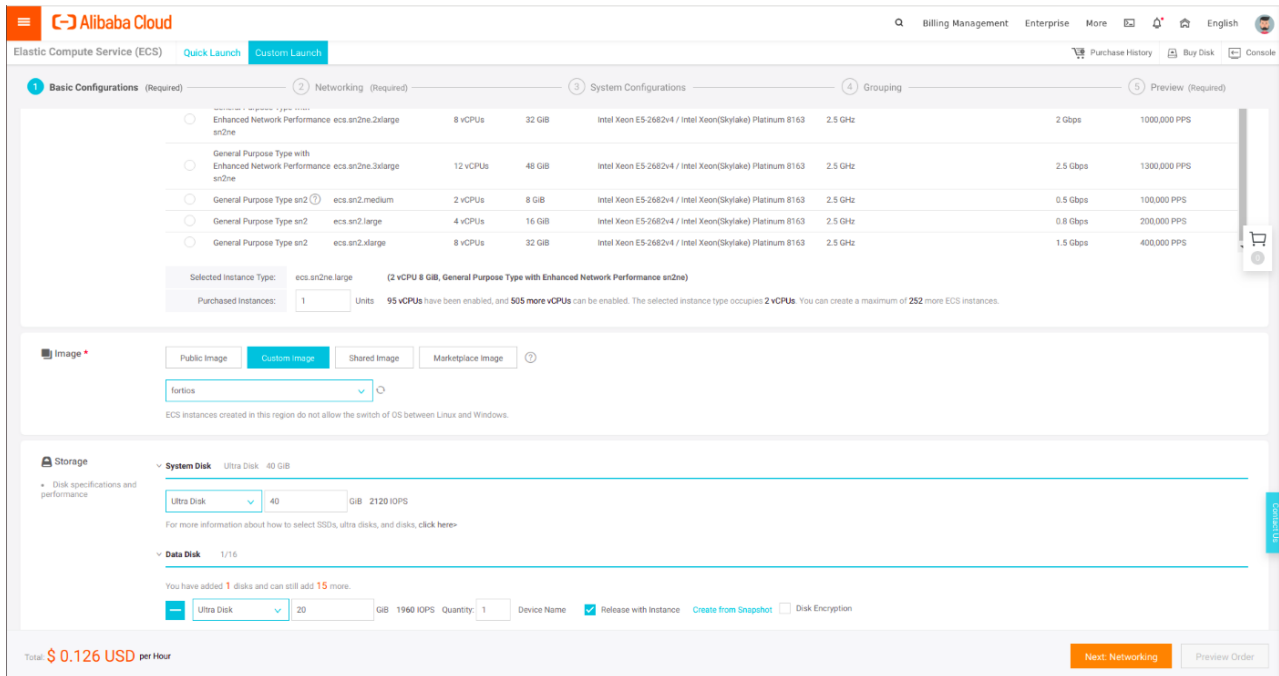
1. Go to *Elastic Computer Service > Instances*, and click *Create Instance*.



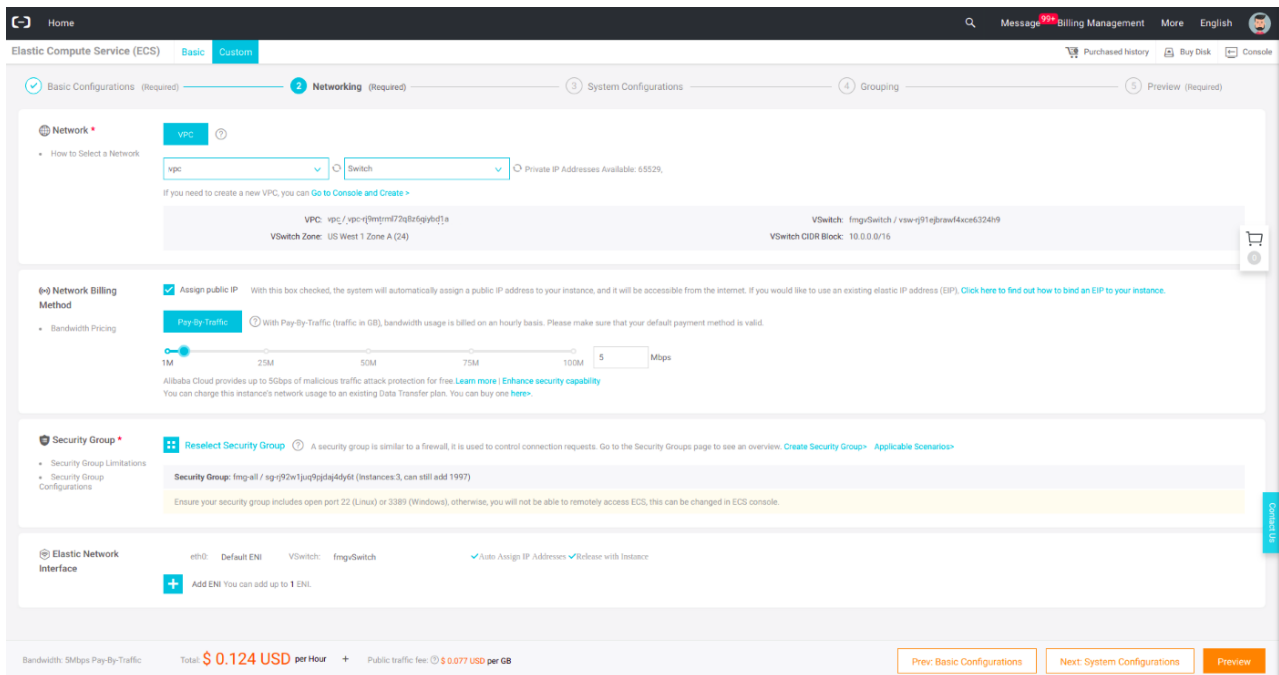
2. Select the *Billing Method, Region, and Instance Type*.



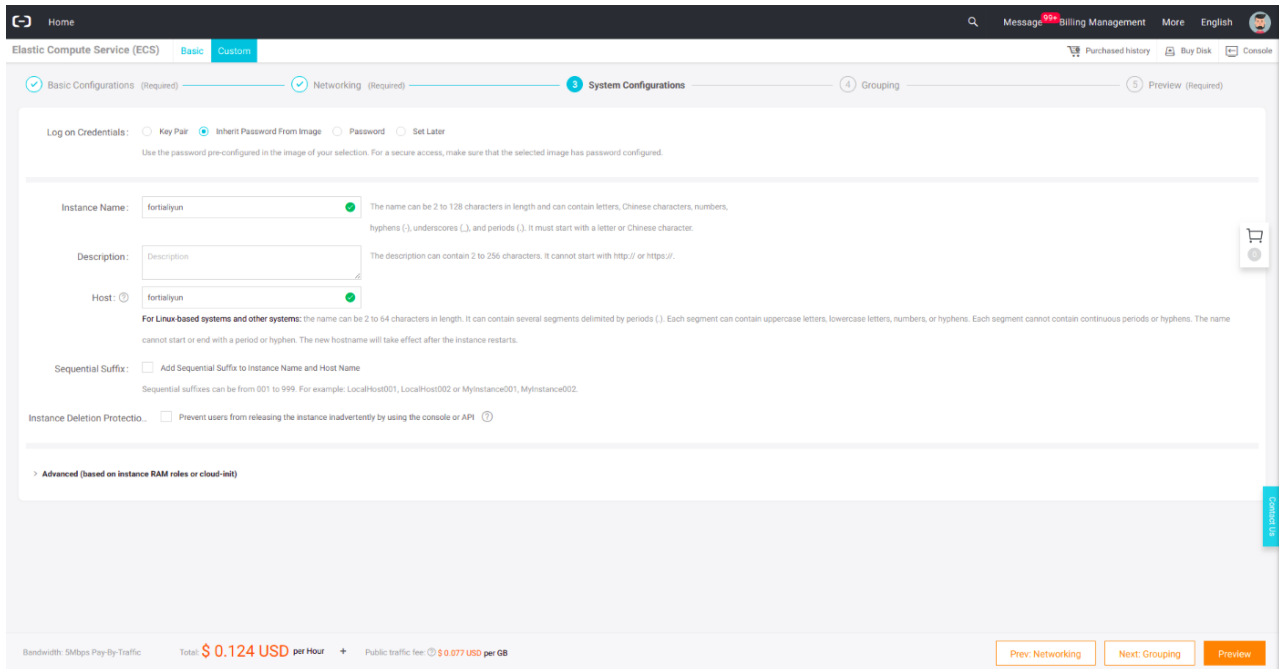
3. Select the *Image* uploaded in [Creating the FortiManager deployment image on page 11](#). If you are deploying FortiManager from the Marketplace, the image is selected automatically. Specify the storage. Create a *System Disk* and a *Data Disk*. Click *Next*.



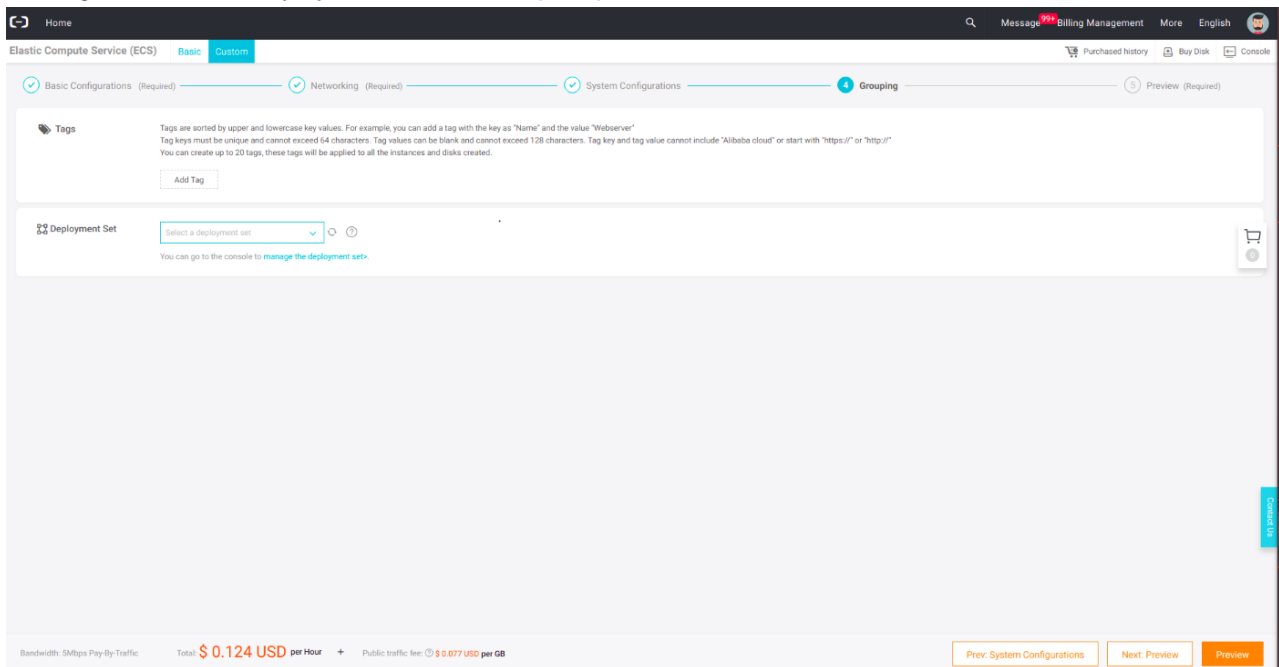
- In **Network**, select the VPC and the Switch created in **Configuring a virtual private cloud** on page 10. In **Network Billing Method**, select **Assign Public IP**. Select the Security Group created in **Creating security groups** on page 13. Click **Next**.



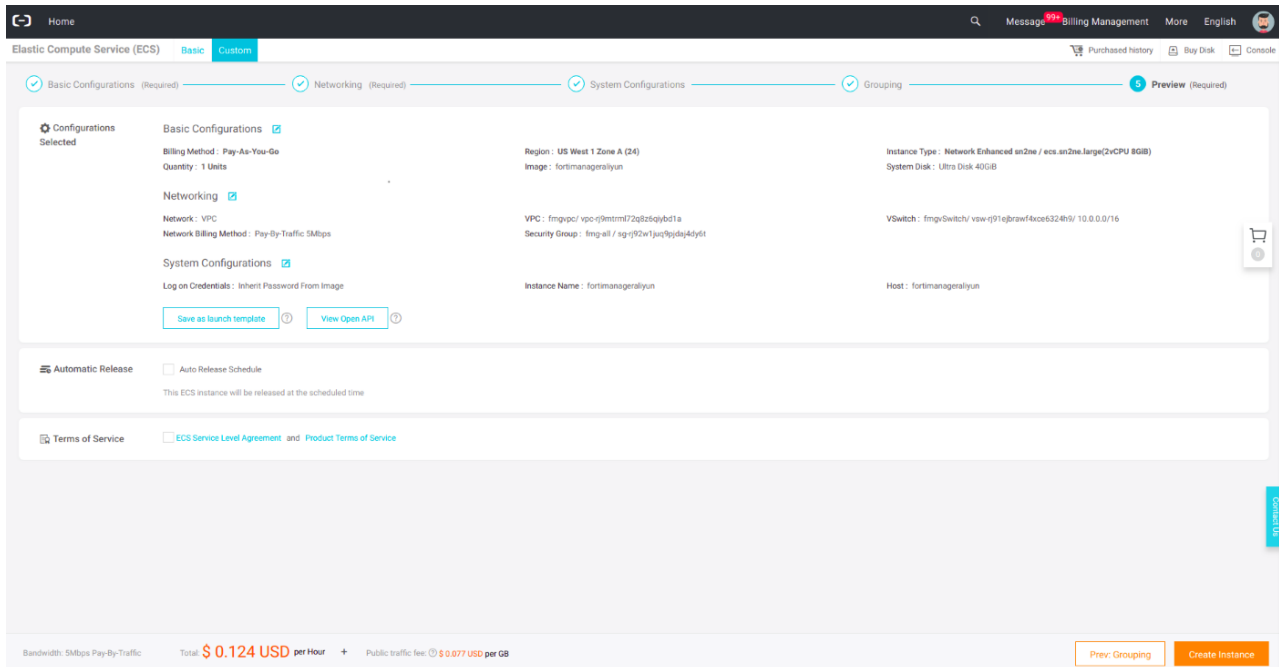
5. Add tags and select a *Deployment Set*. This step is optional. Click *Preview*.



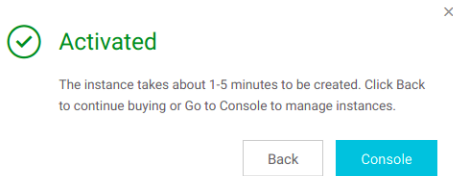
6. Add tags and select a *Deployment Set*. This step is optional. Click *Preview*.



7. Review the configuration, set an *Automatic Release* if required, and accept the *Terms of Service*



8. Click *Create Instance*. The instance takes about 1 to 5 minutes to be created.



Alibaba Cloud can provide you with more preferential and flexible cloud services. See the following documentation:

- [Auto Scaling Service>](#)
- [No fees for stopped instances\(VPC-Connected\)>](#)
- [Switch from Pay-As-You-Go to subscription>](#)
- [Change configurations of Pay-As-You-Go instances>](#)
- [Change EIP Internet bandwidth>](#)

Connecting to the FortiManager-VM

To connect to the FortiManager-VM, you need the public IP address.

The default username is admin and the default password is the AliCloud instance ID, which is represented as a number that you can find after locating the instance in AliCloud console.

To connect to the FortiManager-VM:

1. Click the FortiManager instance and view details to get the public IP address.
2. Locate the instance ID and copy it to the clipboard.
3. In a browser, go to the public IP address for the FortiManager instance.

4. Enter the following information, and press `Enter`:
 - Login: admin
 - Password: Paste the instance ID from the clipboard.You are logged into the FortiManager GUI.
5. Change your password by following the prompts.

Security Fabric connector integration with AliCloud

You can use FortiManager to create a Fabric connector for AliCloud, and then install the Fabric connector to FortiOS.

FortiManager Fabric connectors define the connector type and include information for FortiOS to communicate with and authenticate with the products. In some cases the FortiGate must communicate with products through the Fabric connector, and in other cases the FortiGate communicates directly with the products.

FortiOS works with the Fabric connector to communicate with AliCloud.

For information about Fabric connector, see the [Fortinet Document Library](#).



You cannot import a policy package for the Fabric connector from FortiOS to FortiManager.

Following is an overview of creating Fabric connectors for AliCloud using FortiManager:

1. Create a Fabric connector object for AliCloud. See [Creating Fabric connector objects for AliCloud on page 21](#).
2. Import address names from Azure to the Fabric connector. See [Importing address names to a Fabric connector on page 22](#). FortiManager imports the address names and converts them to dynamic firewall address objects. The objects do not include IP addresses and display in *Firewall Objects > Addresses*.
3. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for AliCloud. See [Creating an IP address policy on page 22](#).
4. Install the policy package to FortiGate. See [Installing policy packages on page 23](#).
FortiGate communicates with AliCloud to dynamically populate the firewall address objects with IP addresses.

Creating Fabric connector objects for AliCloud

With FortiManager, you can create a Fabric connector for AliCloud and import address names from AliCloud to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGates, FortiOS uses the information and the Fabric connector to communicate with AliCloud and dynamically populate the objects with IP addresses.

When you create a Fabric connector for AliCloud, you specify how FortiOS can communicate with AliCloud through the Fabric connector. As a result, you are configuring communication and authentication information for the Fabric connector.

If you enable ADOMs, you can create multiple Fabric connectors per ADOM. However, each Fabric connector requires a unique IP address.

This configuration requires the following:

- FortiManager with ADOM 6.4 or later.
The method that this topic describes for creating Fabric connectors requires ADOM version 6.4 or later.
- FortiManager is managing the FortiGate.
- You have configured the managed FortiGate to work with AliCloud.

To create a Fabric connector for AliCloud:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard displays.
3. Under *SDN*, select *Alibaba Cloud Service*, and click *Next*. The *Alibaba Cloud Service* screen displays.
4. Configure the following options, and then click *OK*:

Name	Enter a name for the Fabric connector object.
Type	Displays Alibaba Cloud Service (ACS).
AccessKey ID	Specify the Fabric connector access key ID.
AccessKey Secret	Specify the Fabric connector access key secret.
Region ID	Specify the Fabric connector region ID.
Update Interval (s)	Specify the update interval for the Fabric connector. Select one of the following options: <ul style="list-style-type: none"> • <i>Use Default</i> to use the default interval. • <i>Specify</i> and specify the interval.
Status	Toggle <i>On</i> to enable the Fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

Importing address names to a Fabric connector

After you configure a Fabric connector, you can import dynamic objects from cloud platforms, such as AliCloud, to the Fabric connector, and dynamic firewall address objects are automatically created.

To import address names for AliCloud:

1. Go to *Policy & Objects > Object Configurations*.
2. Go to *Security Fabric > Fabric Connectors*.
3. In the content pane, right-click the AliCloud Fabric connector, and select *Import*. The *Import SDN Connector* dialog displays.
4. Select the address names, and click *Import*. FortiManager imports the address names and converts them to dynamic firewall address objects that display on the *Firewall Objects > Addresses* pane.

Creating an IP address policy

The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.



On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.

Create New IPv4 Policy

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/>
Outgoing Interface	<input type="text" value="any"/>
Source Internet Service	<input type="checkbox" value="OFF"/>
Source Address	<input type="text" value="all"/>
Source User	<input type="text" value="+"/>
Source User Group	<input type="text" value="+"/>
Source Device	<input type="text" value="+"/>
Destination Internet Service	<input type="checkbox" value="OFF"/>
Destination Address	<input type="text" value="all"/>
Service	<input type="text" value="ALL"/>
Schedule	<input type="text" value="always"/>
Action	<input type="button" value="Deny"/> <input type="button" value="Accept"/> <input type="button" value="IPSEC"/>
Log Traffic	<input checked="" type="checkbox"/> Log Violation Traffic
	<input type="checkbox"/> Generate Logs when Session Starts
Comments	<input type="text"/>
Meta Fields >	
Advanced Options >	

5. Complete the options.
6. Click *OK* to create the policy.
You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Installing policy packages

When installing a policy package, objects that are referenced in the policy will be installed to the target device. Default or per-device mapping must exist or the installation will fail.



Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

To install a policy package to a target device:

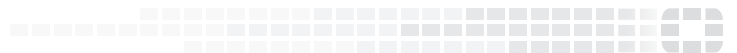
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.

Change log

Date	Change Description
2020-04-09	Initial release.



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.